Performance Work Statement

Risk Management & Internal Control Services

8 June 2026

Revision History

Revision Number	Date	Change and Rationale	Approved By
0	8 June 2026	Initial	

Table of Contents

1.0 GENERAL SCOPE 4
1.1 Background 4
1.2 Scope 4
1.3 Period of Performance 4
1.4 Call Order Tailoring (BPA Execution) 4
2.0 APPLICABLE DOCUMENTS 5
3.0 SITE OPERATIONS 5
3.1 Operating Location / Place of Performance 5
3.2 Security Requirements 5
3.3 Information Technology (IT) and Government Systems 6
3.4 Facility Access and Badging 6
4.0 CORE PERFORMANCE REQUIREMENTS 6
4.1 Risk Assessment & Planning ..... Error! Bookmark not defined.
4.2 Control Testing & Evaluation ..... Error! Bookmark not defined.
4.3 Workpapers, Evidence, and Data Handling ..... Error! Bookmark not defined.
4.4 Deficiency Identification and Reporting ..... Error! Bookmark not defined.
4.5 Corrective Action Support (as directed) ..... Error! Bookmark not defined.
4.6 Assurance Statement Support ..... Error! Bookmark not defined.
4.7 Repository and Collaboration Discipline ..... Error! Bookmark not defined.
4.8 Quality Control of Performance ..... Error! Bookmark not defined.
5.0 KEY PERSONNEL AND PERSONNEL REQUIREMENTS 6
5.1 Key Personnel ..... Error! Bookmark not defined.
5.1.1 Program Manager ..... Error! Bookmark not defined.
5.1.2 RMIC Technical Lead ..... Error! Bookmark not defined.
5.2 Personnel Qualifications ..... Error! Bookmark not defined.
5.3 Personnel Roster ..... Error! Bookmark not defined.
6.0 CALL ORDER WORK PLAN 6
7.0 BPA-LEVEL PROGRAM MANAGEMENT REVIEW (PMR) 6
APPENDIX A - CDRLs 11
APPENDIX B - ACRONYMS 11

1.0 GENERAL SCOPE

1.1 Background

The Defense Intelligence Agency (DIA) requires comprehensive support to maintain, test, and enhance its Enterprise Risk Management (ERM) and Risk Management and Internal Control (RMIC) program, hereforth referred to as RMIC including, but not limited to, Internal Control over Reporting (ICOR) for Management Operations (ICOR-O), Financial Reporting (ICOR-FR), Financial Systems (ICOR-FS), ERM, and payment integrity. This Blanket Purchase Agreement (BPA) provides enterprise-wide RMIC support to assist DIA in maintaining compliance with DoDI 5010.40, OMB Circular A-123 and applicable DoD FIAR guidance/methodology.

This BPA is for non-personal services. Contractor personnel shall perform as contractor employees and shall not be subject to Government supervision or control. Contractor personnel will support but not replace the government-designated Component RMIC manager, required by DoDI 5010.40.

This BPA establishes broad, enterprise-level performance requirements. Specific scope, deliverables, schedules, systems, and performance measures will be defined in individual call orders.

1.2 Scope

The Contractor shall provide sufficient qualified personnel, methodologies, and management necessary to support DIA's RMIC assessment and testing activities across DIA organizations, including performance within highly classified and compartmented environments, as required by the Government.

1.3 Period of Performance

The BPA ordering period shall consist of one (1) 12-month base period with four (4) 12-month option periods. Individual call orders issued under this BPA will specify their own Period of Performance (including start and end dates and any option periods, as applicable) within the BPA ordering period. The Government may elect not to exercise an option period In Accordance With (IAW) the terms of the BPA and applicable contract provisions.

1.4 Call Order Tailoring (BPA Execution)

Individual call orders issued under this BPA will define the specific scope of work, including (as applicable): supported DIA organization(s), locations, systems and networks, applicable RMIC, testing cycles, deliverables and formats, schedules and suspense dates, Government-furnished

resources and access, and acceptance criteria. The Contractor shall perform IAW the requirements established in each call order.

2.0 APPLICABLE DOCUMENTS

The Contractor shall perform all services IAW applicable Federal and Department of Defense (DoD) laws, regulations, standards, and guidance. At a minimum, and as applicable to the work performed under this BPA and individual call orders, the Contractor shall comply with the following:

a. Office of Management and Budget (OMB) Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control
b. Government Accountability Office (GAO), Standards for Internal Control in the Federal Government (Green Book)
c. GAO, Financial Audit Manual (FAM)
d. GAO, Financial Information Systems Control Audit Manual (FISCAM)
e. GAO, A Framework for Managing Fraud Risks in Federal Programs (GAO 15-593SP)
f. DoD Instruction 5010.40, DOD Enterprise Risk Management and Risk Management and Internal Control Program
g. Federal Managers' Financial Integrity Act of 1982 (FMFIA)
h. Payment Integrity Information Act (PIIA)
i. OMB Circular A-136, Financial Reporting Requirements
j. Committee of Sponsoring Organizations of the Treadway Commission (COSO), Internal Control—Integrated Framework
k. National Institute of Standards and Technology (NIST) Cybersecurity Framework and applicable NIST guidance

Note: Where a call order identifies additional governing documents, system-specific policies, or organization-specific procedures, the Contractor shall comply with those requirements for that call order.

3.0 SITE OPERATIONS

3.1 Operating Location / Place of Performance

Unless otherwise authorized in writing by the Government, all work under this BPA and associated call orders shall be performed on-site at Government facilities in the National Capital Region (NCR) and/or other DIA locations as specified in the applicable call order. Due to classified system access requirements, remote performance is not authorized unless explicitly approved in writing by the Government.

3.2 Security Requirements

Contractor personnel shall comply with all DIA security policies and procedures and all requirements specified in the DD Form 254 and the applicable call order. Contractor personnel

shall possess and maintain a Top Secret clearance with Sensitive Compartmented Information (SCI) access (TS/SCI) prior to beginning performance. Additional access requirements (e.g., polygraph, SAP/SAR compartments) will be specified at the call-order level.

3.3 Information Technology (IT) and Government Systems

The Contractor shall use only Government-authorized information systems, networks, and software to process Government information. The Contractor shall not introduce or connect non-Government devices, media, hardware, or software to Government systems without prior written authorization from the Government. The Contractor shall comply with Government direction regarding account provisioning, privileged access, and cybersecurity controls.

3.4 Facility Access and Badging

Contractor personnel shall obtain and maintain appropriate facility access credentials (badges) IAW DIA procedures and shall comply with all access control requirements. Contractor personnel shall immediately report lost, stolen, or damaged badges and shall return all Government-issued badges, credentials, and access devices upon separation from the contract or as otherwise directed by the Government.

4.0 CORE PERFORMANCE REQUIREMENTS

The Contractor shall perform the following core requirements as directed by the Government and as specified in each call order.

4.1 Risk Assessment & Planning

The Contractor shall support DIA in conducting periodic risk assessments across all RMIC domains, identifying key risks, key controls, and control owners. The Contractor shall develop draft test plans, test scripts, sampling methodology, and test schedules for Government review and approval. The Contractor shall support maintaining DIA's risk profile and risk register (IAW DIA guidance), documentation for DoD-level enterprise risk profiles, GAO audit recommendation tracking, and top DoD management challenges, as directed.

4.2 Control Testing & Evaluation

The Contractor shall perform design and operating effectiveness testing of internal controls across all RMIC domains IAW applicable standards including GAO FISCAM (system controls) and GAO FRM Framework (fraud risks). Testing shall include entity-level controls, service provider controls (System and Organization Controls 1 Type 2), and cybersecurity controls. Testing shall be executed only IAW Government-approved test plans, sampling methodology, and test schedules.

4.3 Workpapers, Evidence, and Data Handling

The Contractor shall develop and maintain complete, traceable workpapers and evidence packages sufficient to support conclusions and enable independent re-performance. The Contractor shall maintain chain-of-custody documentation and handle, store, transmit, and dispose of Government information IAW contract security requirements, DoDI 5015.02, and DoD Manual 5200.01 (Volume 3). The Contractor shall not alter production data; any data transformation shall be documented and original extracts preserved.

4.4 Deficiency Identification and Reporting

The Contractor shall document control gaps, exceptions, and deficiencies identified during testing and maintain an up-to-date exception/deficiency log. The Contractor shall identify and classify deficiencies as material weaknesses (MWs) or significant deficiencies (SDs) by RMIC domain, conduct root cause analysis, and prepare draft findings packages (criteria/condition/cause/effect, evidence references, severity rationale, recommended remediation). The Contractor shall promptly notify the Government of potential SDs, MWs, fraud risks, or immediate risks IAW call order requirements.

4.5 Corrective Action Support (as directed)

When directed by the Government, the Contractor shall support development and refinement of Corrective Action Plans (CAPs) including milestones and validation/re-test support. The Contractor shall support tracking and reporting of CAP status, risks, dependencies, and impediments, including coordination with Senior Accountable Officials (SAOs), Assessable Unit Managers (AUMs), and governance bodies (FGB, DPIC, DMAG) as specified in the call order.

4.6 Assurance Statement Support

The Contractor shall assist in preparation of the annual Statement of Assurance (SOA) and compile artifacts, supporting documentation, and executive summaries to support DIA annual assurance reporting requirements across all RMIC domains and applicable ICOR categories (financial reporting and operations), as directed by the Government.

4.7 Repository and Collaboration Discipline

The Contractor shall develop and maintain an internal control document library and use the Government-designated repository (e.g., SharePoint, Advana, or other Government-approved platform) as the official location for workpapers, evidence indexes, logs, and deliverables. The Contractor shall comply with Government direction regarding folder structure, naming conventions, version control, access permissions, and records management IAW DoDI 5015.02.

4.8 Repository and Collaboration Discipline

The Contractor shall establish, implement, and maintain a Quality Control (QC) program to ensure performance is executed IAW Government-approved methodologies and applicable standards. The Contractor shall perform independent QC reviews of testing workpapers and evidence packages prior to submission and shall implement corrective actions to prevent

recurrence of performance deficiencies. When required by an individual call order, the Contractor shall develop and submit a Quality Control Plan (QCP) aligned to the Government-provided QASP within the timeframe specified in the call order. The QCP, if required, will be formalized as a DD Form 1423 CDRL at the call-order level.

5.0 KEY PERSONNEL AND PERSONNEL REQUIREMENTS

5.1 Key Personnel

The Contractor shall identify the following Key Personnel at the BPA level:

a. Program Manager (PM)
b. Risk Management and Internal Control (RMIC) Technical Lead

The Government must approve all Key Personnel prior to the start of performance. The Contractor shall not remove or replace Key Personnel without prior written Government approval, except when necessitated by circumstances beyond the Contractor's control (e.g., illness, death, resignation, or termination of employment).

5.1.1 Program Manager

The Contractor shall provide a PM with:

(1) A bachelor's degree in accounting, finance, business, information systems, or a related field
(2) A minimum of 10 years of experience supporting Federal financial management, internal control, audit readiness/audit support, and/or risk management programs
(3) A minimum of five (5) years of experience managing teams and schedules for complex Federal professional services efforts
(4) A Project Management Professional (PMP) certification is preferred.

Serves as the primary Contractor point of contact for BPA-level execution and governance; responsible for staffing oversight, schedule coordination, issue escalation, and coordination with Government representatives across active call orders.

5.1.2 RMIC Technical Lead

The Contractor shall provide a RMIC Technical Lead with:

(1) A bachelor's degree in accounting, finance, information systems, cybersecurity, or a related field
(2) A minimum of seven (7) years of experience supporting Federal internal control (e.g., OMB Circular A-123), internal control testing, and/or financial statement audit support
(3) Demonstrated knowledge of applicable standards and guidance, including DoDI 5010.40, OMB Circular A-123, GAO Green Book, and GAO FISCAM

(4) At least one of the following certifications is required: CPA, CIA, CISA, CGFM, CGAP, or CDFM

Provides technical leadership for internal control testing methodology and workpaper/evidence quality across active call orders and ensures performance is executed IAW Government-approved methodologies and applicable standards.

5.2 Personnel Qualifications

The Contractor shall provide sufficient qualified personnel to perform the requirements of this BPA and associated call orders. Personnel performing internal controls work shall possess demonstrated knowledge of applicable internal control standards and guidance (e.g., OMB Circular A-123, GAO Green Book, and GAO FISCAM as applicable).

5.3 Personnel Roster

The Contractor shall maintain and provide a BPA-level Personnel Roster identifying all contractor personnel supporting the BPA and active call orders. The roster shall include, at a minimum: individual name, labor category/role, supported call order(s), work location, clearance/access status (e.g., TS/SCI and any additional accesses as applicable), start/end dates on the effort, and qualifications. The Contractor shall submit the roster initially and update it upon personnel changes, as directed by the Government.

6.0 CALL ORDER WORK PLAN

For each call order issued under this BPA, the Contractor shall develop and submit a Call Order Work Plan within 15 business days after call order award (or as otherwise directed by the Government). The Call Order Work Plan shall describe the Contractor's approach to accomplishing the call order requirements and shall include, at a minimum:

a. Task approach and assumptions
b. Staffing plan and clearance/access status
c. Schedule with milestones
d. Risks, dependencies, and mitigation actions
e. Quality control approach for performance execution

The Contractor shall update the Call Order Work Plan as directed by the Government.

7.0 BPA-LEVEL PROGRAM MANAGEMENT REVIEW (PMR)

The Contractor shall support a quarterly Program Management Review (PMR) with the Government to review BPA health and performance of active call orders. The PMR shall be scheduled quarterly or as otherwise directed by the Government. The Contractor shall provide a PMR briefing package in advance of the meeting and shall document PMR decisions and action items in an action item log. The Contractor shall track action items to closure and report status at subsequent PMRs.

APPENDIX A - CONTRACT DATA REQUIREMENTS LIST (CDRLs)

The deliverables identified in this Appendix will be formalized through DD Form 1423, Contract Data Requirements Lists (CDRLs). Unless otherwise directed by the Government, deliverables shall be submitted electronically via the Government-designated repository. Specific formats, content requirements, and submission procedures will be confirmed at the call-order level.

CDRL #	Deliverable Name	PWS Ref	Freq	Due Date
	Call Order Work Plan	6.0	As required	Within 15 business days after call order award (or as otherwise directed by the Government)
	Quarterly PMR Briefing Package	7.0	Quarterly	NLT two (2) business days prior to the PMR
	Personnel Roster	5.3	Once and as required	Initial within 10 business days after BPA award; Updates within two (2) business days of personnel changes

APPENDIX B – ACRONYMS

AUM – Assessable Unit Manager
BPA – Blanket Purchase Agreement
CAP – Corrective Action Plan
CDFM – Certified Defense Financial Manager
CDRL – Contract Data Requirements List
CGAP – Certified Government Auditing Professional
CGFM – Certified Government Financial Manager
CIA – Certified Internal Auditor
CISA – Certified Information Systems Auditor
COR – Contracting Officer's Representative
COSO – Committee of Sponsoring Organizations of the Treadway Commission
CPA – Certified Public Accountant
DIA – Defense Intelligence Agency
DoD – Department of Defense
ERM – Enterprise Risk Management
FAM – Financial Audit Manual
FISCAM – Financial Information Systems Control Audit Manual
FMFIA – Federal Managers' Financial Integrity Act of 1982
FRM – Fraud Risk Management
GAO – Government Accountability Office
IAW – In Accordance With
ICOR – Internal Control over Reporting
ICOR-FR – Internal Control over Financial Reporting
ICOR-FS – Internal Control over Financial Systems
ICOR-O – Internal Control over Reporting for Management Operations
IT – Information Technology
MW – Material Weakness
NCR – National Capital Region
NIST – National Institute of Standards and Technology
OMB – Office of Management and Budget
PIIA – Payment Integrity Information Act
PM – Program Manager
PMR – Program Management Review
PMP – Project Management Professional
PWS – Performance Work Statement
QC – Quality Control
QASP – Quality Assurance Surveillance Plan
QCP – Quality Control Plan

RMIC – Risk Management and Internal Control
SAO – Senior Accountable Official
SCI – Sensitive Compartmented Information
SOA – Statement of Assurance
TS/SCI – Top Secret / Sensitive Compartmented Information